PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-224313
(43)Date of publication of application : 17.08.1999

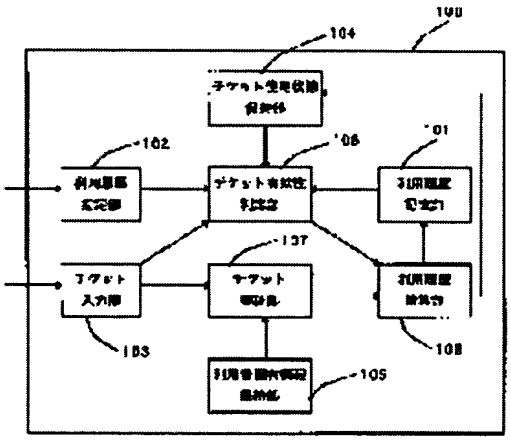
(51)Int.Cl. G06K 17/00
G06F 17/60
G06K 19/10

(21)Application number : 10-027143
(22)Date of filing : 09.02.1998

(71)Applicant : FUJI XEROX CO LTD
(72)Inventor : NAKAGAKI JUHEI
KIKO KENICHIROU
KIYOUJIMA HITOKI
TANIGUCHI SHINICHIRO

(54) ELECTRONIC TICKET SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To perform the settlement of account while using various tickets later by simply recording a utilization history at the time of utilization.
SOLUTION: A ticket validity discriminating part 106 discriminates the validity of a ticket while using the using state of the ticket held in a using state holding part 104, inputted additional ticket information and utilization history designated by a utilization history designating part 102. A ticket verifying part 107 verifies the legality of the ticket while using the inputted ticket, user peculiar information, additional ticket information and ticket disclosure information. When the ticket validity discriminating part 106 discriminates the ticket is valid and the ticket verifying part 107 verifies the ticket is legal, a utilization history account settling part 108 regards the input of the legal ticket required for settling the account of the utilization history to which the settlement of account is designated, and the utilization history designated by the utilization history designating part 102 is regarded complete in the settlement of account.



LEGAL STATUS

[Date of request for examination] 20.09.2002
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－224313

(43)公開日　平成11年(1999)８月17日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｋ　17/00		Ｇ０６Ｋ　17/00	Ｔ
			Ｌ
Ｇ０６Ｆ　17/60		Ｇ０６Ｆ　15/21	Ｂ
Ｇ０６Ｋ　19/10		Ｇ０６Ｋ　19/00	Ｒ

審査請求　未請求　請求項の数11　ＯＬ　（全 13 頁）

(21)出願番号　特願平10－27143

(22)出願日　平成10年(1998)２月９日

(71)出願人　000005496
富士ゼロックス株式会社
東京都港区赤坂二丁目17番22号

(72)発明者　中垣　寿平
神奈川県足柄上郡中井町境430　グリーンテクなかい　富士ゼロックス株式会社内

(72)発明者　木子　健一郎
神奈川県足柄上郡中井町境430　グリーンテクなかい　富士ゼロックス株式会社内

(72)発明者　京嶋　仁樹
神奈川県足柄上郡中井町境430　グリーンテクなかい　富士ゼロックス株式会社内

(74)代理人　弁理士　澤田　俊夫

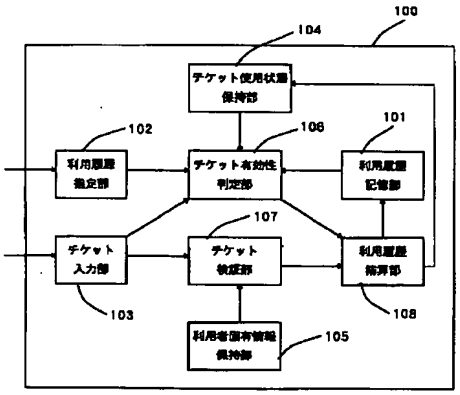
最終頁に続く

(54)【発明の名称】　電子チケットシステム

(57)【要約】

【課題】　利用時には、単に、その利用履歴を記録しておき、後に、種々のタイプのチケットを用いて精算する。

【解決手段】　チケット有効性判定部１０６は、使用状態保持部１０４に保持されているチケットの使用状態と、入力されたチケット付加情報と、利用履歴指定部１０２により指定された利用履歴とを用いてチケットの有効性を判定する。チケット検証部１０７は、入力されたチケットと利用者固有情報とチケット付加情報とチケット公開情報とを用いてチケットの正当性を検証する。利用履歴精算部１０８は、チケット有効性判定部１０６によりチケットが有効であると判定され、かつチケット検証部１０７によりチケットが正当であると検証されたときに、精算を指定された利用履歴を精算するのに必要な正当なチケットが入力されたものとみなし、利用履歴指定部１０２により指定された利用履歴を精算済みとする。



第１の実施例における電子チケットシステムの構成

1

【特許請求の範囲】

【請求項１】　利用履歴を記憶する利用履歴記憶手段と、

精算する上記利用履歴を指定する利用履歴指定手段と、

精算に使用するチケットを入力するチケット入力手段と、

利用者固有情報を保持する利用者固有情報保持手段と、

上記チケットの有効性を判定するチケット有効性判定手段と、

上記チケットと上記利用者固有情報とを用いて上記チケットの正当性を検証するチケット検証手段と、

上記チケット有効性判定手段により上記チケットが有効であると判定され、かつ上記チケット検証手段により上記チケットが正当であると検証されたときに、上記利用履歴指定手段により指定された利用履歴を精算済みとする利用履歴精算手段とを有することを特徴とする電子チケットシステム。

【請求項２】　請求項１に記載の電子チケットシステムであって、

上記チケット入力手段は、さらにチケットを識別するチケット識別子を含んで上記チケットを入力し、

さらに上記チケットの使用状態を上記チケット識別子と対応づけて記憶するチケット使用状態保持手段を有し、

上記チケット有効性判定手段は、上記使用状態保持手段に保持されている上記チケットの使用状態を用いて有効性の判定を行うことを特徴とする電子チケットシステム。

【請求項３】　請求項１または２に記載の電子チケットシステムであって、

上記チケット入力手段は、上記チケットの利用条件を示すチケット付加情報を含んで上記チケットを入力し、

上記チケット有効性判定手段は、さらに上記チケット付加情報と上記利用履歴指定手段により指定された上記利用履歴とを判定材料に加えて上記チケットの有効性を判定し、

上記チケット検証手段は、上記チケットと上記利用者固有情報と上記チケット付加情報とを用いて上記チケットの正当性を検証することを特徴とする電子チケットシステム。

【請求項４】　請求項１～３のいずれかに記載の電子チケットシステムであって、

上記チケット入力手段は、さらに上記チケットの作成に用いたチケットの秘密情報に対応するチケットの公開情報を含んで上記チケットを入力し、

上記チケット検証手段は、上記チケットと上記利用者固有情報と上記チケット付加情報と上記チケットの公開情報とを用いて上記チケットの正当性を検証することを特徴とする電子チケットシステム。

【請求項５】　請求項４に記載の電子チケットシステムであって、上記チケット検証手段は、上記チケットと上記利用者固有情報と上記チケット付加情報と上記チケットの公開情報とを用いて上記チケットの秘密情報を算出し、上記チケットの秘密情報と上記チケットの公開情報とが対応していることを確認することをもって上記チケットが正当であると判定することを特徴とする電子チケットシステム。

2

【請求項６】　利用履歴を記憶する利用履歴記憶手段と、

精算する上記利用履歴を指定する利用履歴指定手段と、

精算に使用するチケットの利用条件を示すチケット付加情報とチケットの公開情報とチケットを識別するチケット識別子とを入力するチケット利用条件入力手段と、

乱数を生成し出力する乱数生成手段と、

上記出力した乱数と精算に使用するチケットとにより計算された証明情報を入力する証明情報入力手段と、

利用者固有情報を保持する利用者固有情報保持手段と、

上記チケットの使用状態を上記チケット識別子と対応づけて記憶するチケット使用状態保持手段と、

上記チケット付加情報と上記利用履歴指定手段により指定された上記利用履歴と上記チケット使用状態保持手段に保持されている上記チケットの使用状態とを用いてチケットの有効性を判定するチケット有効性判定手段と、

入力された上記証明情報と上記利用者固有情報と上記チケット付加情報と上記チケットの公開情報と上記乱数とを用いて上記チケットの正当性を検証するチケット検証手段と、

上記チケット有効性判定手段により上記チケットが有効であると判定され、かつ上記チケット検証手段により上記チケットが正当であると検証されたときに、上記利用履歴指定手段により指定された利用履歴を精算済みとする利用履歴精算手段とを有することを特徴とする電子チケットシステム。

【請求項７】　請求項１～６のいずれかに記載の電子チケットシステムであって、上記電子チケットシステムは、内部のデータおよび処理手続きを外部から観測することを困難ならしめる防御手段中に保持されていることを特徴とする電子チケットシステム。

【請求項８】　請求項１～７のいずれかに記載の電子チケットシステムであって、上記電子チケットシステムは、ＩＣカードなどの携帯可能な小型演算装置として構成されていることを特徴とする電子チケットシステム。

【請求項９】　請求項１～８のいずれかに記載の電子チケットシステムであって、

上記電子チケットシステムは、さらにチケット発行装置を有し、

上記チケット発行装置は、

上記利用者固有情報を保持する発行装置側利用者固有情報保持手段と、

上記チケットの秘密情報を保持するチケット秘密情報保持手段と、

上記チケット付加情報を保持するチケット付加情報保持手段と、
上記発行装置側利用者固有情報保持手段に保持している上記利用者固有情報と上記チケット秘密情報保持手段に保持している上記チケットの秘密情報と上記チケット付加情報保持手段に保持している上記チケット付加情報とを用いてチケットを発行することを特徴とする電子チケットシステム。
【請求項１０】　利用履歴が記憶された機器を用いて料金を精算する料金精算方法において、
精算する利用履歴を指定する利用履歴指定ステップと、
精算に使用するチケットを入力するチケット入力ステップと、
上記チケットの有効性を判定するチケット有効性判定ステップと、
上記チケット有効性判定ステップにおいて上記チケットが有効であると判定されときに、上記利用履歴指定ステップにおいて指定された利用履歴を精算済みとする利用履歴精算ステップとを有することを特徴とする料金精算方法。
【請求項１１】　利用履歴を記憶する利用履歴記憶ステップと、
精算する上記利用履歴を指定する利用履歴指定ステップと、
精算に使用するチケットを入力するチケット入力ステップと、
利用者固有情報を保持する利用者固有情報保持ステップと、
上記チケットの有効性を判定するチケット有効性判定ステップと、
上記チケットと上記利用者固有情報とを用いて上記チケットの正当性を検証するチケット検証ステップと、
上記チケット有効性判定ステップにおいて上記チケットが有効であると判定され、かつ上記チケット検証ステップにおいて上記チケットが正当であると検証されたときに、上記利用履歴指定ステップにおいて指定された利用履歴を精算済みとする利用履歴精算ステップとを有することを特徴とする料金精算方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、チケットやカードの作成、発行および利用の技術に関し、とくにチケットを用いて料金を精算する技術に関する。
【０００２】
【背景技術】［従来の技術］乗車券、通行券、入場券、指定券、予約券、回数券、定期券、商品券、プリペイドカード、ポイントカード、会員証、通行証、許可証などは、それを保持する利用者が、それに応じた各々の権利を保持することを証明する。ここでは、これらをまとめてチケットと呼ぶ。一般にチケットは、権利を与える者

もしくはその代理人（以下ではまとめて発行者と呼ぶ）が発行して、利用者が保持管理する。従来、チケットは、紙やプラスチックなどへ印刷やエンボス加工などの処理を施すことで実現されていた。
【０００３】このようなチケットをここでは紙チケットと呼ぶ。これに対して、近年では、発行者が利用者に与えた権利を特定できて、正しいチケットであることを検証できるという機能を持つ電子チケットを実現する試みがなされている。電子情報は、作成が容易であり、通信回線を通して送信できるという特徴を持つ。しかしながら、完全なコピーを簡単に作れるので、電子チケットを実現するには、偽造と複製による不正利用への対策が必要である。電子署名の技術を用いることにより偽造は防止できるが、複製の防止は困難であり、複製による不正利用を防止することが、電子チケットの実現にあたっての最大の課題となっていた。
【０００４】この問題に対する、解決策として、従来、チケットの利用時に正当な利用者か確認する第１の従来技術、発行者以外の者にチケットを複写する機会を与えない第２の従来技術、検証時の通信を公開できるように第２の従来技術を修正した第３の従来技術の３つの方法が提案されてきた。
【０００５】第１の従来技術は、チケットの利用時に、利用者が正当な利用者かどうかを確認する方法であり、利用者は、チケットを利用する時に、チケットとともに自分が利用者特定情報に適合する正当な利用者であることを示す。利用者特定情報に適合していれば、対応する権利の行使が認められる。確認のために必要な情報（利用者特定情報）と、与えた権利とを対応づける情報がチケットとして発行され、利用者が記録管理する。発行者以外の者が勝手にチケットを偽造できないようにするためには、発行者がチケットに電子署名を施す。電子署名のないチケットは、偽造されたものと判断される。利用者特定情報には、身元、顔写真などの身体的特徴、パスワードなどの知識の所有、などが利用できる。
【０００６】しかしながらこの方法では、利用する利用者特定情報に応じて、いくつかの問題点が生ずる。
【０００７】例えば、利用者特定情報に利用者の身元を利用する方法では、発行時と検証時に利用者の身元が明らかになり、匿名性が失われてしまう。また、通信回線を利用した遠隔的な環境で身分を安全に証明する方法は実現されていないので、このような環境では正当な権利を持たないものが、不当にチケットを利用することを防止することができない。
【０００８】利用者特定情報にパスワードを利用すれば、匿名性の問題は軽減されるが、パスワードを記憶する負荷を利用者にあたえる。また、利用者が故意にパスワードを漏洩させることを防止できないので、不正利用の危険が増してしまうという問題点もある。
【０００９】第２の従来技術は、例えば特開平８－１４

７５００号公報に示されるようなものであり、発行者以外の者にチケットを複写する機会を与えない方法である。この方法では、利用者が保持管理しているチケットを複写できないようにする機構と、発行時や検証時の通信からチケットが漏洩しない機構の両方を必要とする。

【００１０】しかしながら、この方法では、（１）発行者以外の者はチケットを複写できないので、チケットの正当性を第三者に証明することが困難になる、（２）チケットの発行時と検証時の通信の内容も機密に行うので、チケットの発行時と検証時にプライバシーなどの利用者の権利が侵害されていないことを証明できない、といった問題点が生ずる。

【００１１】第３の従来技術は、例えば特公平６－５２５１８号公報に示されるようなものであり、検証時の通信を公開できるように第２の従来技術を修正した方法である。この方法では、第２の従来技術と同様に、チケットを秘密情報として利用者の所持する装置（証明器）に複写できないように記録するが、検証の方法が異なる。まず、検証を行う検証器は、証明器に乱数などの繰り返し利用されない値（チャレンジ）を送る。証明器は、チケットである秘密情報を利用した演算をチャレンジに対して施して、得られた値（レスポンス）を検証器に送り返す。検証器は、秘密情報とチャレンジを利用してレスポンスが演算されたことを確認することで、利用者の正当性を認証する。レスポンスから逆に秘密情報を求めることを計算量的に困難とすることで、チャレンジとレスポンスを秘密通信とする必要がなくなる。

【００１２】この方法は、認証のために利用されるものであり、正当なチケットを保持しているか否か以外に情報を伝達しない。このため、有効期限などを示すことができず、単純なチケットしか表現できない。また、チケットを証明器に送信する方法が、第２の従来技術と同様に機密通信で行う必要があり、不当に利用者の情報を開示して利用者の権利を侵害していないことを証明できないという問題があった。

【００１３】このように、従来の技術はいずれも、チケットに必要な不正利用を防止する機能を実現するために、第三者に対するチケットの内容証明の機能や利用者の匿名性を犠牲にしている点に問題があった。

【００１４】［関連技術］これらの問題を解決する関連技術として、特願平９－１８８０６４号（平成９年７月１４日出願、未公開）に示す方法が提案されている。この方法では、各利用者に、固有情報を封入した証明装置を持たせ、チケットはその証明装置固有情報とチケットの秘密情報とから生成して発行する。検証時には、検証装置が乱数などを用いて発行した値（チャレンジ）に対して、証明装置がチケットを用いて値（レスポンス）を検証器に送り返すことによって、正当なチケットを保持しているかどうかの検証を行う。正当なチケットと正当な証明装置の組みあわせのみが、正当なレスポンスを計

算することが可能になる。

【００１５】この方法では、チケットは秘密情報が取り出せないように構成されており、また他の証明装置と組にして利用しようとしても、利用できないようになっている。また、証明装置が検証装置に送る値（レスポンス）には、利用者が持つ証明装置の証明装置固有情報や利用者自身の情報は含まれることがないように構成できるので、利用者の匿名性も保つことが可能である。さらに、検証は、公開情報のみを用いて行うことが可能なので、利用者自身や第三者がチケットの正当性を確認することが可能である。

【００１６】このように、この関連技術の方法を使うと、電子チケットの基本的な機能をすべて満たした安全な電子チケットを実現することができ、上記の問題をすべて解決することが可能である。

【００１７】ところで、この関連技術では、検証器がチケットを特定する情報を証明器に送る事により、検証器が検証しようとするチケットが証明器の中で一意に定まる事を前提としている。しかし、実際には、その検証器で検証可能なチケットが証明器内に複数存在する事も考えられる。そのような場合には、検証の途中で選択肢が複数あることを示し、利用者に選択してもらうなどの処理を行うことを想定している。しかし、その検証器で検証可能なチケットが証明器内に複数存在し、かつその場で利用者が選択できないこともある。

【００１８】たとえば、鉄道の乗車券のようなものを考えた場合、その駅から有効な回数券や定期券など複数のチケットが証明器の中に存在する事がありうる。そのような場合、証明器では、どのチケットを利用者が利用しようとしているのか判断する事ができない。また、鉄道の場合、自動改札機による処理にすると、短時間に大勢の人が通過できるようにしなければならないため、改札機による検証の途中で、利用者にチケットの選択を促すというような処理を行うことはできない。また、改札機を通る前に、利用者に予め利用するチケットを選択しておいてもらうということも、選択を忘れる利用者は少なからずいることが予想されるため、困難である。

【００１９】そこでこのような場合には、検証器が検証しようとするチケットが証明器の中で一意に定まるようにする必要がある。

【００２０】チケットが証明器の中で一意に定まるようにするには、何でも検証できる万能のチケットを１枚だけ証明器の中に保持しておき、検証の際にはその万能チケットを用いて検証を行い、検証の履歴を証明器の中に残すようにすればよい。そして、その精算はプリペイドのような前払い方式か、あるいは一定期間毎に履歴を回収して精算する後払い方式を取るようにすればよい。

【００２１】しかし、このような方式を採用した場合、チケットを予め購入することによって行われていたディスカウントなどの機能が失われることになる。たとえ

ば、定期券や回数券などのボリュームディスカウントや、半年前に購入すると５０%引きで、３ヶ月前なら３０%引きというような前売りによるディスカウントなどの機能である。

【００２２】

【発明が解決しようとする課題】そこで、本発明では、例えば、万能チケットを用いて検証を行い、検証の履歴を証明器の中に残すような場合の精算時において、チケットを予め購入することによって行われていたディスカウントなどの機能を失うことなく、精算可能にすることを課題とする。もちろん、万能チケットを用いた場合だけでなく、一般に利用の履歴を記録して、その記録を精算する際にも、使える精算機能であってもよい。

【００２３】

【課題を解決するための手段】本発明では、上記の課題を解決するために、電子チケットシステムに、利用履歴を記憶する利用履歴記憶手段と、精算する上記利用履歴を指定する利用履歴指定手段と、精算に使用するチケットを入力するチケット入力手段と、利用者固有情報を保持する利用者固有情報保持手段と、上記チケットの有効性を判定するチケット有効性判定手段と、上記チケットと上記利用者固有情報とを用いて上記チケットの正当性を検証するチケット検証手段と、上記チケット有効性判定手段により上記チケットが有効であると判定され、かつ上記チケット検証手段により上記チケットが正当であると検証されたときに、上記利用履歴指定手段により指定された利用履歴を精算済みとする利用履歴精算手段とを設けるようにしている。

【００２４】この構成においては、利用時には、単に、その利用履歴を記録しておき、後に、チケットを用いて精算するので、利用時の操作が少なくなる。また、精算時にチケットの有効性を判断するので、チケットの利用条件やディスカウントを反映させて精算を行なうことができる。

【００２５】

【発明の実施の態様】以下、本発明の実施例について説明する。

［第１の実施例］第１の実施例では、回数券を表すチケットで利用履歴を精算する例について説明する。この実施例の電子チケットシステムは、例えばＩＣカードとして実現され、利用者はそのＩＣカードを持って何らかのサービスを利用し、その利用履歴をＩＣカード中に記録する。そして後で、自宅のパソコンなどにそのＩＣカードを挿入し、パソコン上に保持しているチケットを用いて、利用履歴の精算を行う。利用履歴を記録する手法は、利用の許可を行う検証器側と何らかの認証を行い、その結果として記録されるのが望ましいが、利用したことが正しく反映されていれば何でもよい。例えば、この認証の手段としてチケットを用いてもよい。チケットを用いる方法としては、先の特願平９－１８８０６４号に示す方法や、特願平１０－０２７０７４号に示す方法を用いてもよい。特願平９－１８８０６４号は検証器側と証明器側との間で相互認証し、証明器の保持者にサービス等を提供し、そのサービスに応じて証明器の内部状態（利用履歴）を書き込み更新できるようにしている。また、特願平１０－０２７０７４号では、相互認証に加え、検証器側で、証明器から提示されたチケットの判定を行ない、間違ったチケットの提示や不正なチケットの提示により証明器の内部状態が変更されないようにしている。

【００２６】この場合、利用・履歴記憶時に第１のチケットを使い、また、精算時に第２のチケットを使う。以下の説明は精算時のチケットに関するものである。

【００２７】図１は、本発明の第１の実施例の電子チケットシステムを全体として示しており、この図において、電子チケットシステム１００は、利用履歴記憶部１０１、利用履歴指定部１０２、チケット入力部１０３、チケット使用状態保持部１０４、利用者固有情報保持部１０５、チケット有効性判定部１０６、チケット検証部１０７、利用履歴精算部１０８を含んで構成される。

【００２８】利用履歴記憶部１０１は、利用の履歴を記憶する部分である。利用の履歴は、例えば自動改札機などにより改札がなされたときに、書き込まれるものである。利用履歴指定部１０２は、利用履歴記憶部１０１に記憶されている利用履歴の中から、チケットにより精算する利用履歴を指定するものである。チケット入力部１０３は、精算するのに使用するチケットを入力する部分である。本実施例では、チケットとともに、チケットを識別するチケット識別子と、チケットの利用条件を示すチケット付加情報と、チケットの作成に用いたチケットの秘密情報に対応するチケットの公開情報とを入力する。

【００２９】チケット使用状態保持部１０４は、チケットの使用状態をチケット識別子と対応づけて記憶する。チケットの使用状態とは、例えば今までにそのチケットを使用した回数などである。これを用いて、例えば、回数券の使用回数をカウントしておき、その回数券の使用限度になるとそれ以上、使用できないような処理を行う。また、回数券以外でも、同じチケットの再利用を防止する意味からも用いられる。

【００３０】利用者固有情報保持部１０５は、利用者毎に個別に割り当てられた利用者の固有情報を保持する。利用者固有情報は、ＩＣカードなどの中に秘密に封入されており、利用者自身も読み出すことはできない。

【００３１】チケット有効性判定部１０６は、チケットの有効性を判定する。より具体的には、チケット有効性判定部１０６は、使用状態保持部１０４に保持されているチケットの使用状態と、入力されたチケット付加情報と、利用履歴指定部１０２により指定された利用履歴とを用いてチケットの有効性を判定する。例えば、回数券

チケットのチケット付加情報に記載されている回数上限と使用状態保持部１０４に保持されているチケットの使用回数とを比較して上限を超えていないかで判定したり、チケット付加情報に記載されている乗車可能区間と精算する利用履歴として記録されている実際の乗車区間とを比較したり、チケット付加情報に記載されているチケットの有効期間と精算する利用履歴として記録されている実際の使用日時とを比較したりして判定する。

【００３２】チケット検証部１０７は、入力されたチケットと利用者固有情報とチケット付加情報とチケット公開情報とを用いてチケットの正当性を検証する。

【００３３】利用履歴精算部１０８は、チケット有効性判定部１０６によりチケットが有効であると判定され、かつチケット検証部１０７によりチケットが正当であると検証されたときに、精算を指定された利用履歴を精算するのに必要な正当なチケットが入力されたものとみなし、利用履歴指定部１０２により指定された利用履歴を精算済みとする。精算済みとする方法としては、単に利用履歴を利用履歴記憶部１０１から削除してもよいし、利用履歴記憶部１０１で記憶している各利用履歴に未精算か精算済みかを示すフラグを持たせ、対応する履歴の精算済みのフラグを立てるようにしてもよい。

【００３４】次に本実施例の動作を図４のフローチャートを参照しながら具体例を挙げて詳細に説明する。この説明では、チケットの作成時に用いるチケット秘密情報として、公開鍵暗号方式のＲＳＡ（Ｒｉｖｅｓｔ－Ｓｈａｍｉｒ－Ａｄｌｅｍａｎ）暗号を用いた例について説明する。

【００３５】ＲＳＡ暗号では、ｐ、ｑを大きな素数、ｎを法数、Ｅを公開鍵、Ｄを秘密鍵とするとき、以下の関＊係が成り立つ。ｐ、ｑを大きな素数、ｎを法数とするとき、

【００３６】

【数１】

$$n = pq$$

$$ED \equiv 1 \mod (p-1)(q-1)$$

このうち、素数ｐ、ｑは秘密に作成して、チケットの作成が終了し次第、秘密のまま破棄してしまう。

【００３７】本実施例では、具体例として、横浜－藤沢間の鉄道に乗車した利用履歴を、回数券チケットで精算する場合について説明する。

【００３８】今、利用履歴記憶部１０１の内容が図２のようになっているとする。このうちの、Ｎｏ（通し番号）が２１４の履歴を、回数券で精算する。上述したＲＳＡを用いて、チケット秘密情報をＤ、チケット公開情報を（Ｅ，ｎ）とし、利用者固有情報をｄｕ、チケット付加情報をＬとする。この時、チケット入力部１０３から入力されるチケットｔは以下のような形式である。

【００３９】

【数２】$t = D - F(n, L, du)$

ここで、関数Ｆ（）は一方向性関数であり、一方向性ハッシュ関数ＭＤ５、ＳＨＡや、共通鍵暗号ＤＥＳ（Ｄａｔａ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）などを用いることができる。

【００４０】チケット付加情報Ｌには、利用可能区間、有効期間、回数上限などが記載されており、今それらの情報は以下のようになっている。

【００４１】

【表１】

利用可能区間：	横浜－藤沢
有効期間：	１９９７．５．１～１９９７．１０．３１
回数上限：	１１回

上記のようなチケット付加情報をＬ３０１とし、このＬ３０１を用いて発行されたチケットをｔ３０１とする。利用者固有情報をｄ００３とし、このチケットに用いられているチケット秘密情報をＤ０１、対応するチケット公開情報を（Ｅ０１，ｎ０１）とすると、発行されるチケットｔ３０１は以下のようになる。

【００４２】

【数３】

$$t301 = D01 - F(n01, L301, d003)$$

このチケットは現在３回使用されているとすると、チケット使用状態保持部は図３に示すように、チケット識別子が００３の使用回数が「３」となっている。

【００４３】さて、今、横浜－藤沢間の鉄道に乗車した利用履歴を、回数券チケットで精算するために、利用履歴指定部１０２からＮｏ．２１４の履歴が指定され、チケット入力部１０３から、チケットｔ３０１とチケット付加情報Ｌ３０１とチケット識別子００３とチケット公開情報（Ｅ０１，ｎ０１）とが入力されたとする（図４のステップＳ１１）。するとチケット有効性判定部１０６は、利用履歴記憶部１０１から指定されたＮｏ．２１４の履歴を読み出し、チケット付加情報Ｌ３０１と比較する（Ｓ１２、Ｓ１３）。Ｎｏ．２１４の履歴の利用区間は横浜－藤沢間であり、利用日時は「９７．９．１０」である。一方、チケット付加情報Ｌ３０１の利用可能区間も横浜－藤沢間であり、有効期間は１９９７．５．１～１９９７．１０．３１であることから、利用可能区間、有効期間ともにチケットの利用は可能である。

【００４４】次に、チケット有効性判定部１０６は、チケット使用状態保持部１０４からチケット識別子００３の使用状態を読み出し、チケット付加情報Ｌ３０１と比較する。チケット識別子００３の使用状態（ここでは使用回数）は3回であり、チケット付加情報Ｌ３０１の回数上限は１１回であるので、チケットの利用は可能である。ここで、チケット使用状態保持部１０４から読み出

した使用回数が１１回を示していた場合は、チケットは使用不能であると判定する。

【００４５】上述の２つのチケット有効性の判定により、チケットの利用は可能であるので、チケット有効性判定部１０６はチケットを有効であると判定する。

【００４６】次にチケット検証部１０７による検証を行う。チケット検証部１０７は、利用者固有情報保持部１０５から利用者固有情報ｄ００３を読み出し、チケット入力部１０３から入力されたチケットｔ３０１とチケット付加情報Ｌ３０１とチケット公開情報（Ｅ０１，ｎ０１）とを用いて検証を行う（Ｓ１４、Ｓ１５）。

【００４７】検証は例えば以下の方法で行う。

【００４８】ある整数ａを生成し、ａの法ｎのもとでの［ｔ＋Ｆ（ｎ，Ｌ，ｄｕ）］・Ｅによるべき乗を計算し、ａと等しくなるかどうかで検証する。

【００４９】

【数４】

$$a^{[t+F(n,L,du)]\cdot E} \mod n = ? \quad a \qquad (1)$$

正しいチケットと正しい利用者固有情報を用いれば、

【００５０】

【数５】

$$[t+F(n,L,du)] = D-F(n,L,du)+F(n,L,du) = D$$

であるので、

【００５１】

【数６】

$$a^{[t+F(n,L,du)]\cdot E} \mod n = a^{DE} \mod n = a$$

と計算でき、（１）式が成立するはずである。

【００５２】（１）式の左辺に、各値を代入すると、＊

$$[a^{t}a^{F(n,L,du)}]^{E} \mod n = ? \quad a \qquad (2)$$

本実施例では、回数券の例について説明したが、チケットが定期券の時には、回数のチェックはせずに、読み出した利用履歴を用いて区間と有効期間から有効性を判定すればいい。また、回数に関係のない場合でも、チケット使用状態保持部から読み出したチケットの使用状態の情報を用いることで、一度しか使えないチケットを再使用することを防ぐことができる。

【００６０】また、本実施例では、ＲＳＡ公開鍵暗号方式を用いて説明したが、これに限定するものではない。例えば離散対数系の暗号方式も使用することが可能である。

【００６１】例えば、ｐは素数であり、Ｇは離散対数問題が困難な有限群であり、ｇは有限群Ｇの位数ｐの元であり、

【００６２】

【数８】

$$y = g^{x} \mod p$$

が満たされるとき、（ｐ，Ｇ，ｇ，ｙ）を公開の情報とし、ｘを秘密の情報とする。実際には、Ｇを有限体の乗法群として構成したり、有限体上の楕円曲線として構成することができる。

【００６３】このとき、（Ｇ，ｇ）をシステム共通とし、公開情報（ｙ，ｐ）、秘密情報ｘとして、チケットを

【００６４】

【数９】

$$t = x - F(y,L,du)$$

として構成することができる。ここで、関数ＦやＬやｄｕなどは、ＲＳＡの時と同様である。

【００６５】検証は、（３）式が成立するかどうかで行えばよい。

【００６６】

【数１０】

$$g^{[t+F(y,L,du)]} \mod p = ? \quad y \qquad (3)$$

正しいチケットと正しい利用者固有情報を用いれば、

【００６７】

＊【００５３】

【数７】

$$a^{[t301+F(n01,L301,d003)]\cdot E01} \mod n01 = a^{001\cdot E01} \mod n01 - a$$

となり、（１）式が成り立つので、チケットは正当であると検証される。

【００５４】以上により、チケット有効性判定部１０６によりチケットが有効であると判定され、チケット検証部１０７によりチケットは正当であると検証されたので、利用履歴精算部１０８は、指定された利用履歴を精算済みと処理する。つまり、利用履歴精算部１０８は、利用履歴記憶部１０１に記憶されているＮｏ．２１４の履歴の精算記録の欄を、未精算から精算済みに変更する（Ｓ１６）。

【００５５】さらに、利用履歴精算部１０８は、チケット使用状態保持部１０４のチケット識別子が００３の使用回数を１だけ増やして４に変更する（同じくＳ１６）。

【００５６】なお、図４のステップＳ１２の有効性判別において有効でないと判別された場合や、ステップＳ１４において検証が失敗した場合には精算が行なわれず、エラー等が表示される（Ｓ１７）。

【００５７】以上で、チケットによる利用履歴の精算処理は終了する。精算終了後の利用履歴記憶部の内容例を図５に示す。

【００５８】本実施例では、チケットの正当性の検証に、（１）式を用いて検証したが、（２）式を用いてもよい。どちらも結果は同じである。

【００５９】

【数８】

13

【数１１】

$$[t+F(y, L, du)] = x - F(y, L, du) + F(y, L, du) = x$$

であるので、

【００６８】

【数１２】

$$g^{[t+F(y,L,du)]} \mod p = g^{x} \mod p = y$$

と計算でき、（３）式が成立するはずである。チケットの式は、

【００６９】

【数１３】 $t = x - F(p, L, du)$

のようにしても構わない。

【００７０】［第２の実施例］以下、本発明の実施例について説明する。

【００７１】図６は、本発明の第２の実施例の電子チケットシステムを全体として示す図であり、図６において、電子チケットシステム１００は、利用履歴記憶部１０１、利用履歴指定部１０２、チケット利用条件入力部１０９、チケット使用状態保持部１０４、利用者固有情報保持部１０５、チケット有効性判定部１０６、チケット検証部１０７、利用履歴精算部１０８、乱数生成部１１０、証明情報入力部１１１を含んで構成される。

【００７２】チケット利用条件入力部１０９は、利用するチケットに関連する条件などを入力する部分である。＊

$$[r^{t} r^{F(n,L,du,t-id)}]^{E} \mod n = ?\ r \qquad (4)$$

（４）式の左辺のr^{t}は、証明情報入力部１１１から入力された値を用いる。左辺のそれ以外の部分は、チケット利用条件入力部１０９から入力された値と利用者固有情報保持部１０５に保持している値を用いて計算する。

【００８０】本実施例におけるチケットｔは以下のような形式である。※

$$\begin{aligned} r^{t} r^{F(n,L,du,t-id)}]^{E} \mod n &= [r^{D-F(n,L,du,t-id)} r^{F(n,L,du,t-id)}]^{E} \mod n \\ &= [r^{D-F(n,L,du,t-id)+F(n,L,du,t-id)}]^{E} \mod n \\ &= [r^{D}]^{E} \mod n \\ &= r^{DE} \mod n \\ &= r \end{aligned}$$

つまり、（４）式の左辺と右辺とが等しくなり、（４）式が成り立つ。

【００８３】第１の実施例と異なり、一方向性関数Ｆ（）の中にチケット識別子ｔ－ｉｄを入れているのは、チケット識別子だけを入れ替えるような偽造を防ぐためである。この偽造は第１の実施例でも行われる可能性があるので、第１の実施例でも同様の形式にしてもよい。

【００８４】これ以外は第１の実施例と同様であるので、説明を繰り返さない。

14

＊本実施例では、チケットを識別するチケット識別子と、チケットの利用条件を示すチケット付加情報と、チケットの作成に用いたチケットの秘密情報に対応するチケットの公開情報とを入力する。

【００７３】乱数生成部１１０は、乱数を生成し、出力する。

【００７４】証明情報入力部１１１は、乱数生成部１１０が出力した乱数と精算に使用するチケットとにより計算された証明情報を入力する。清算に使用するチケットは、本電子チケットシステムの外部で保持されており、そのチケットを用いて証明情報が計算される。

【００７５】例えば、乱数生成部１１０が乱数ｒを生成したとし、精算に使用するチケットがｔ、法数がｎであるとすると、証明情報入力部１１１からは、

【００７６】

【数１４】 $r^{t} \mod n$

が入力される。

【００７７】他の部分は第１の実施例と同様に構成される。

【００７８】乱数生成部１１０が出力した乱数をｒ、精算に使用するチケットをｔ、一方向性関数をＦ（）、チケット公開情報を（Ｅ，ｎ）、チケット付加情報をＬ、利用者固有情報をｄｕ、チケット識別子をｔ－ｉｄとすると、第２の実施例における検証は（４）式が成立するかどうかで検証する。

【００７９】

【数１５】

$$[r^{t} r^{F(n,L,du,t-id)}]^{E} \mod n = ?\ r \qquad (4)$$

※【００８１】

【数１６】 $t = D - F(n, L, du, t-id)$

正しいチケットと正しい利用者固有情報を用いれば、（４）式の左辺は、以下のように計算される。

【００８２】

【数１７】

$$\begin{aligned} r^{t} r^{F(n,L,du,t-id)}]^{E} \mod n &= [r^{D-F(n,L,du,t-id)} r^{F(n,L,du,t-id)}]^{E} \mod n \\ &= [r^{D-F(n,L,du,t-id)+F(n,L,du,t-id)}]^{E} \mod n \\ &= [r^{D}]^{E} \mod n \\ &= r^{DE} \mod n \\ &= r \end{aligned}$$

【００８５】この実施例においては、チケット自体を入力することなく、乱数生成部１１０が出力した乱数に対してチケットでべき乗を行った計算結果を入力するようにしている。一般に、べき乗の計算は大きな計算量を必要とする。チケットｔの長さ（ビット長）は大きくなることが考えられるため、r^{t}の計算には大きな計算量が必要となる。

【００８６】この実施例では、このr^{t}の計算を一般に貧弱な計算能力しか持たないＩＣカードで行わずに、外部のパーソナルコンピュータの計算リソースを用いて行

うように構成することができ、第１の実施例の（２）式を使う場合に比べて高速な検証を可能にすることができる。

【００８７】

【発明の効果】以上説明したように、本発明によれば、利用時には、単に、その利用履歴を記録しておき、後に、チケットを用いて精算するので、利用時の操作が少なくなる。また、精算時にチケットの有効性を判断するので、チケットの利用条件やディスカウントを反映させて精算を行なうことができる。

【図面の簡単な説明】

【図１】　第１の実施例における電子チケットシステムの構成を示すブロック図である。

【図２】　第１の実施例における利用履歴記憶部の内容の例を示す図である。

【図３】　第１の実施例におけるチケット使用状態保持部の内容の例を示す図である。

【図４】　第１の実施例における処理の流れを示すフロ＊ーチャートである。

【図５】　第１の実施例における精算終了後の利用履歴記憶部の内容の例を示す図である。

【図６】　第２の実施例における電子チケットシステムの構成を示すブロック図である。

【符号の説明】

１００　電子チケットシステム
１０１　利用履歴記憶部
１０２　利用履歴指定部
１０３　チケット入力部
１０４　チケット使用状態保持部
１０５　利用者固有情報保持部
１０６　チケット有効性判定部
１０７　チケット検証部
１０８　利用履歴精算部
１０９　チケット利用条件入力部
１１０　乱数生成部
１１１　証明情報入力部

【図２】

No	入場記録	出場記録	精算記録
211	...	...	...
212	97.9.5, 13:15　藤沢	97.9.5, 13:31　辻堂	未精算
213	97.9.8, 15:30　横浜	97.9.8, 16:21　東京	精算済み
214	97.9.10, 10:21　横浜	97.9.10, 10:55　藤沢	未精算
215	97.9.10, 18:17　藤沢	97.9.10, 18:28　辻堂	未精算
216	97.9.16, 12:15　藤沢	97.9.16, 12:29　辻堂	未精算
217	...	...	...

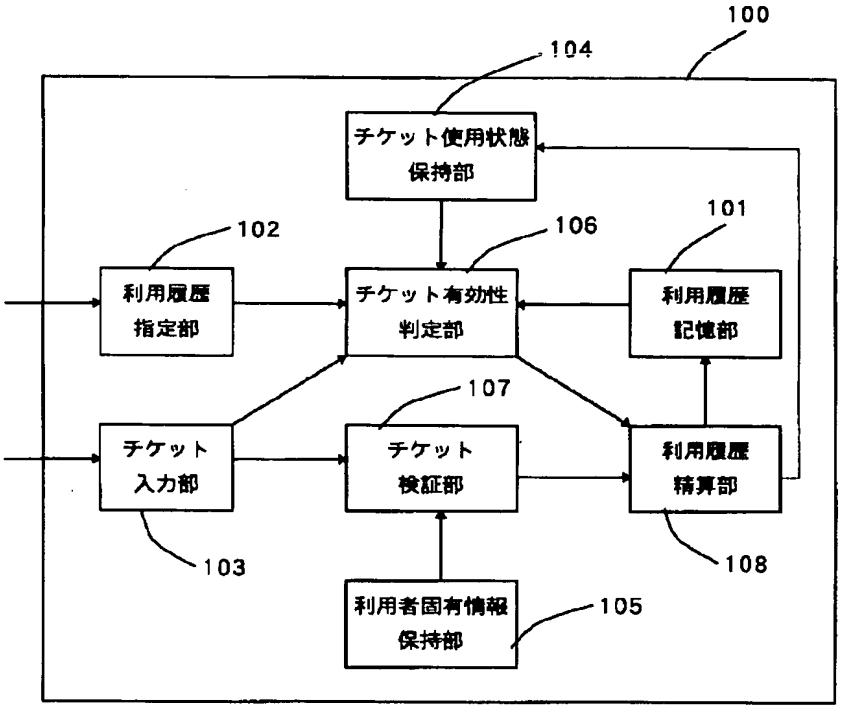
第１の実施例における利用履歴記憶部の例

【図３】

チケット識別子	使用回数
001	5
002	1
003	3
004	1
...	...
...	...

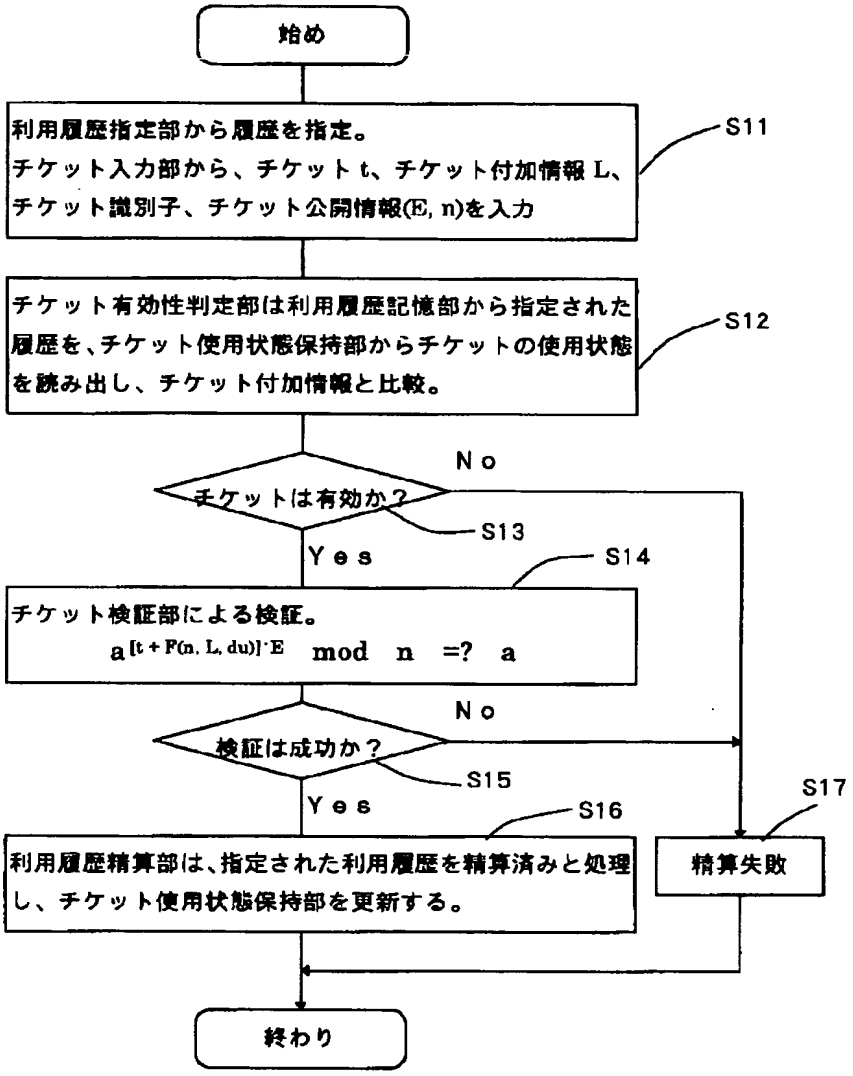
第１の実施例におけるチケット使用状態保持部の例

【図１】



第１の実施例における電子チケットシステムの構成

【図４】



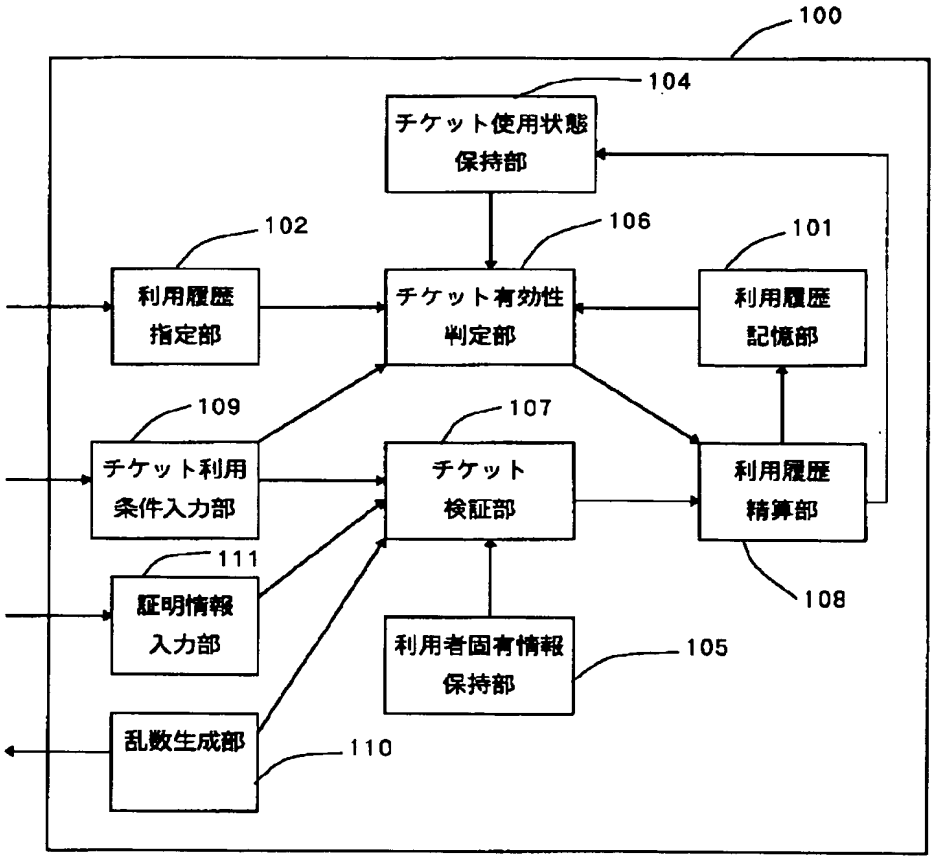
第１の実施例における処理の流れ

【図５】

No	入場記録	出場記録	精算記録
211	...	...	...
212	97.9.5, 13:15　藤沢	97.9.5, 13:31　辻堂	未精算
213	97.9.8, 15:30　横浜	97.9.8, 16:21　東京	精算済み
214	97.9.10, 10:21　横浜	97.9.10, 10:55　藤沢	精算済み
215	97.9.10, 18:17　藤沢	97.9.10, 18:28　辻堂	未精算
216	97.9.16, 12:15　藤沢	97.9.16, 12:29　辻堂	未精算
217	...	...	...

第１の実施例における精算終了後の利用履歴記憶部の例

【図６】



第２の実施例における電子チケットシステムの構成

フロントページの続き

(72)発明者　谷口　慎一郎
神奈川県足柄上郡中井町境430　グリーンテクなかい　富士ゼロックス株式会社内